PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-031980
(43)Date of publication of application : 28.01.2000

(51)Int.Cl. H04L 12/28
G06F 13/00
H04Q 7/38
H04L 9/36

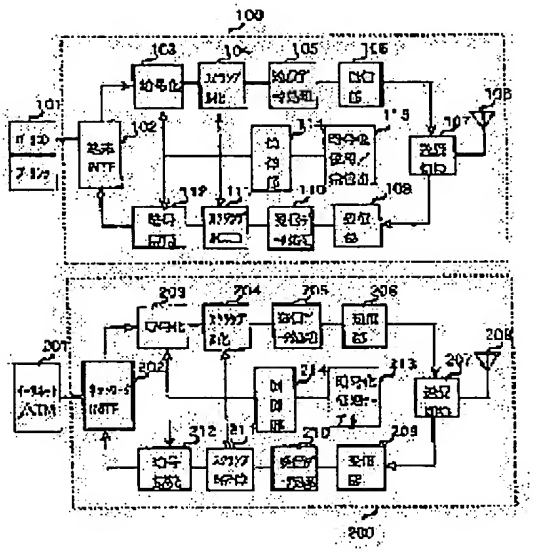
(21)Application number : 10-195484
(22)Date of filing : 10.07.1998

(71)Applicant : KOKUSAI ELECTRIC CO LTD
NIPPON TELEGR & TELEPH CORP <NTT>

(72)Inventor : MURAKAMI HIROYUKI
OKINO EMI
MIURA SHUNJI
SUZUKI YOSHIFUMI

(54) RADIO LAN SYSTEM AND ENCIPHERING METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the processing of data not to be enciphered from being delayed and to enable communication without causing any unpleasantness due to processing delay by providing an encryption use/unuse selecting part for selecting the use/unuse of encryption by a user, providing a master station with a management table for managing a slave station and enciphering only data to be enciphered.
SOLUTION: A slave station control part 114 operates a slave station transmission data encryption processing part 103 and enciphers input data when an encryption use/unuse selecting part 113 selects encryption use. A slave station transmission data scrambling processing part 104 makes the enciphered input data random, a slave station transmission data processing part 105 makes it a packet and a slave station transmitting part 106 performs radio modulation of it. When a signal showing that encryption processing is performed is included in a received signal, a master station controlling part 214 registers that the terminal selects encryption with an encryption management table 213 and a master station received data encryption decoding processing part 212 performs encryption decoding processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－31980
（P2000－31980A）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/00	３１０Ｂ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｌ	５Ｊ１０４
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０３３
Ｈ０４Ｌ　9/36		Ｈ０４Ｌ　9/00	６８５	５Ｋ０６７

審査請求　未請求　請求項の数２　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－195484

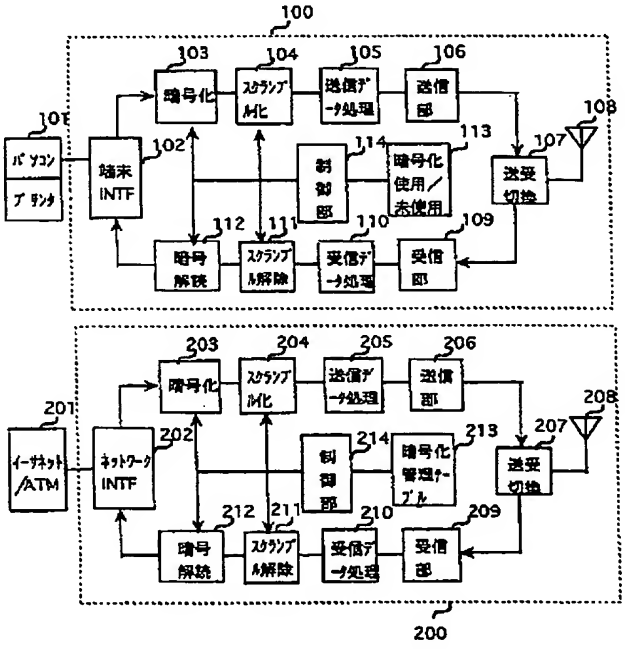
(22)出願日　平成10年７月10日(1998.7.10)

(71)出願人　000001122
国際電気株式会社
東京都中野区東中野三丁目14番20号
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　村上　博行
東京都中野区東中野三丁目14番20号　国際電気株式会社内
(74)代理人　100093872
弁理士　高崎　芳紘

最終頁に続く

(54)【発明の名称】　無線ＬＡＮシステムとその暗号化方法

(57)【要約】
【課題】　親局と複数の子局からなる無線ＬＡＮシステムで、無線区間からの傍受を防ぐための暗号化を、処理時間増大のためのデータ伝送のスループットの低下、通信の遅れによる不快感をなるべく生じないようにする。
【解決手段】　子局に暗号化を行うか行わないかの選択ができるスイッチを設け、ユーザは、送信データが暗号化を必要とするデータかどうかを判断して、暗号化が必要としたデータ送信の場合にのみ、暗号化を行い、暗号化が不要と判断した場合は、暗号化を行わずにデータを送信し処理の高速化を図る。親局には、管理テーブルを設け子局が暗号化を選択したかどうかを記憶し、親局からのデータ送信は、この管理テーブルに記憶している子局の状態に従って暗号化するかどうかを定める。



1

【特許請求の範囲】

【請求項１】　ネットワークに接続されるネットワーク側の親局とその親局と無線回線で接続される複数の子局とからなる無線ＬＡＮシステムにおいて、

子局は、

少なくとも送信データの作成機能と受信データの処理表示機能を有した端末装置と、その端末装置からの送信データを暗号化するための子局暗号化手段と、送信データの暗号化を行うか否かを選択するための暗号化選択手段と、この手段により暗号化を行う選択がなされているときかつそのときのみ前記子局暗号化手段により送信データが暗号化されるように制御するための子局送信制御手段と、前記送信データまたはそれが暗号化されたデータとそのデータが暗号化されているか否かを示す子局フラグとを含む伝送データを作成して無線信号に変換し送信する子局送信手段と、親局からの無線信号を受信し受信データを取り出す子局受信手段と、前記受信データが暗号化されているときにこれを解読するための子局解読手段と、前記受信データに含まれている親局フラグが当該受信データが暗号化されていることを示しているときかつそのときのみ前記子局解読手段により当該受信データが解読されるように制御するための子局受信制御手段と、を備えており、

親局は、

管理テーブルと、子局からの無線信号を受信して受信データを取り出すための親局受信手段と、前記受信データが暗号化されているときにこれを解読するための親局解読手段と、前記受信データに含まれている子局フラグを前記管理テーブルへ子局対応に格納し、かつその子局フラグが当該受信データが暗号化されていることを示しているときかつそのときのみ前記親局解読手段により当該受信データが解読されるように制御するための親局受信制御手段と、前記受信データまたはそれが解読されたデータをネットワークへ送出しまたネットワークからの送信データを取り込むためのインターフェースと、取り込んだ送信データを暗号化するための親局暗号化手段と、前記管理テーブルの該当する子局フラグが暗号化を示しているときかつそのときのみ当該送信データが前記親局暗号化手段により暗号化されるように制御するための親局送信制御手段と、前記送信データまたはそれが暗号化されたデータとそのデータが暗号化されているか否かを示す親局フラグとを含む伝送データを作成して無線信号に変換し送信する親子局送信手段と、

を備えていることを特徴とする無線ＬＡＮシステム。

【請求項２】　ネットワークに接続されるネットワーク側の親局とその親局と無線回線で接続される複数の子局とからなり、無線回線上では少なくとも送信データを伝送するデータチャネルと、子局から親局にデータの送信を要求する要求チャネルと、親局から子局にデータチャネルでの送信を指示する許可チャネルを含む伝送フレーム構成を有した無線ＬＡＮシステムの暗号化方法であって、

2

ユーザが暗号化の使用／未使用を選択するための暗号化使用／未使用選択部を、親局に子局を管理するための管理テーブルを設けるとともに、

子局から親局へデータ送信する場合、

前記暗号化使用／未使用選択部を見て暗号化使用／未使用を示すフラグを前記要求チャネルに含めて親局へ送信し、

前記要求チャネルを受信した親局では受信した要求チャネルのフラグを前記管理テーブルに当該子局対応で格納し、さらに前記許可チャネルで当該子局へ前記格納したのと同じフラグを含めた許可信号を送信し、

前記許可チャネルで自局への信号を受信した子局では、受信した許可チャネルに含まれているフラグを見て、このフラグが暗号化を示していれば送信データを暗号化したのちそのデータと暗号化を示すフラグとを前記データチャネルで親局へ送信し、前記フラグが暗号化を示していなければ送信データを暗号化せずにそのまま暗号化していないことを示すフラグとともに前記データチャネルで親局に送信し、

前記データチャネルを受信した親局では、その中に含まれるフラグが暗号化を示しているときかつそのときのみ受信したデータの暗号化解読を行い、

親局から子局へデータを送信する場合、

前記管理テーブルの送信先子局に対応するフラグを取り出して前記許可チャネルで許可信号とともに子局へ送信し、またそのフラグが暗号化を示しているときかつそのときのみ送信データを暗号化し、暗号化を示していないときは送信データそのままで前記データチャネルで当該子局へ送信し、

前記許可チャネル及びデータチャネルを受信した子局では、受信した許可チャネルの信号に含まれているフラグが暗号化を示しているときかつそのときのみ前記データチャネルで受信したデータの暗号化解読を行う、

ようにしたことを特徴とする無線ＬＡＮシステムの暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、無線ＬＡＮシステムとその暗号化方法に関するものである。

【０００２】

【従来の技術】従来の無線ＬＡＮシステムのシステム構成図を図２に示す。図２でネットワーク親局装置（単に親局と称す）と、端末側子局装置（単に子局と称す）との間は無線で結ばれ、送受信データはパケット化されている。通常、送受信データにはスクランブル化が施されているが、暗号化は行われていない。

【０００３】

【発明が解決しようとする課題】しかし、現代において

は、携帯電話に代表されるように無線区間から傍受する犯罪が多くなり、送受信データの暗号化が望まれていた。暗号化方式としては、暗号化キーをユーザごとに割り当て、暗号化／解読処理を行うＤＥＳやＦＥＡＬなどが望ましいが、これらの暗号化方式は、処理時間がかかる等の問題がある。このような処理時間がかかる暗号化方式で秘匿する必要がないデータまで暗号化すると、データ伝送のスループットが低下するとともに、通信の遅れで不快感が生ずるという欠点があった。

【０００４】本発明の目的は、暗号化キーによる暗号化を行う場合、処理時間が掛かり、秘匿する必要のないデータまで暗号化し、スループットが低下するという欠点を解決し、秘匿する必要のあるデータのみをユーザが指定して暗号化するようにした無線ＬＡＮシステムとその暗号化方法を提供することにある。

【０００５】

【課題を解決するための手段】上記の目的を達成するために本発明は、ネットワークに接続されるネットワーク側の親局とその親局と無線回線で接続される複数の子局とからなる無線ＬＡＮシステムにおいて、子局は、少なくとも送信データの作成機能と受信データの処理表示機能を有した端末装置と、その端末装置からの送信データを暗号化するための子局暗号化手段と、送信データの暗号化を行うか否かを選択するための暗号化選択手段と、この手段により暗号化を行う選択がなされているときかつそのときのみ前記子局暗号化手段により送信データが暗号化されるように制御するための子局送信制御手段と、前記送信データまたはそれが暗号化されたデータとそのデータが暗号化されているか否かを示す子局フラグとを含む伝送データを作成して無線信号に変換し送信する子局送信手段と、親局からの無線信号を受信し受信データを取り出す子局受信手段と、前記受信データが暗号化されているときにこれを解読するための子局解読手段と、前記受信データに含まれている親局フラグが当該受信データが暗号化されていることを示しているときかつそのときのみ前記子局解読手段により当該受信データが解読されるように制御するための子局受信制御手段と、を備えており、親局は、管理テーブルと、子局からの無線信号を受信して受信データを取り出すための親局受信手段と、前記受信データが暗号化されているときにこれを解読するための親局解読手段と、前記受信データに含まれている子局フラグを前記管理テーブルへ子局対応に格納し、かつその子局フラグが当該受信データが暗号化されていることを示しているときかつそのときのみ前記親局解読手段により当該受信データが解読されるように制御するための親局受信制御手段と、前記受信データまたはそれが解読されたデータをネットワークへ送出しまたネットワークからの送信データを取り込むためのインターフェースと、取り込んだ送信データを暗号化するための親局暗号化手段と、前記管理テーブルの該当する子局フラグが暗号化を示しているときかつそのときのみ当該送信データが前記親局暗号化手段により暗号化されるように制御するための親局送信制御手段と、前記送信データまたはそれが暗号化されたデータとそのデータが暗号化されているか否かを示す親局フラグとを含む伝送データを作成して無線信号に変換し送信する親子局送信手段と、を備えていることを特徴とする無線ＬＡＮシステムを提供する。

【０００６】また、本発明は、ネットワークに接続されるネットワーク側の親局とその親局と無線回線で接続される複数の子局とからなり、無線回線上では少なくとも送信データを伝送するデータチャネルと、子局から親局にデータの送信を要求する要求チャネルと、親局から子局にデータチャネルでの送信を指示する許可チャネルを含む伝送フレーム構成を有した無線ＬＡＮシステムの暗号化方法であって、ユーザが暗号化の使用／未使用を選択するための暗号化使用／未使用選択部を、親局に子局を管理するための管理テーブルを設けるとともに、子局から親局へデータ送信する場合、前記暗号化使用／未使用選択部を見て暗号化使用／未使用を示すフラグを前記要求チャネルに含めて親局へ送信し、前記要求チャネルを受信した親局では受信した要求チャネルのフラグを前記管理テーブルに当該子局対応で格納し、さらに前記許可チャネルで当該子局へ前記格納したのと同じフラグを含めた許可信号を送信し、前記許可チャネルで自局への信号を受信した子局では、受信した許可チャネルに含まれているフラグを見て、このフラグが暗号化を示していれば送信データを暗号化したのちそのデータと暗号化を示すフラグとを前記データチャネルで親局へ送信し、前記フラグが暗号化を示していなければ送信データを暗号化せずにそのまま暗号化していないことを示すフラグとともに前記データチャネルで親局に送信し、前記データチャネルを受信した親局では、その中に含まれるフラグが暗号化を示しているときかつそのときのみ受信したデータの暗号化解読を行い、親局から子局へデータを送信する場合、前記管理テーブルの送信先子局に対応するフラグを取り出して前記許可チャネルで許可信号とともに子局へ送信し、またそのフラグが暗号化を示しているときかつそのときのみ送信データを暗号化し、暗号化を示していないときは送信データそのままで前記データチャネルで当該子局へ送信し、前記許可チャネル及びデータチャネルを受信した子局では、受信した許可チャネルの信号に含まれているフラグが暗号化を示しているときかつそのときのみ前記データチャネルで受信したデータの暗号化解読を行う、ようにしたことを特徴とする無線ＬＡＮシステムの暗号化方法を提供する。

【０００７】

【発明の実施の形態】以下、本発明の実施の形態を詳細に説明する。図１は、本発明になる無線ＬＡＮシステムの構成例を示すブロック図である。この図により構成と

概略動作を説明すると、端末側子局装置１００には、パソコンとプリンタからなる入出力装置１０１が接続され、パソコンからの入力データが端末インタフェース１０２を経由し、子局送信データ暗号化処理部１０３に送られる。子局制御部１１４は、暗号化使用／未使用選択部１１３で暗号化使用が選択されていると、子局送信データ暗号化処理部１０３を動作させ、入力データを暗号化する。暗号化の方法としては、自局に割り当てられた暗号化キーを用いてＤＥＳやＦＥＡＬにより暗号化する。ここで、暗号化使用／未使用選択部１１３は、コードレス電話機などに設けられているスクランブル選択スイッチと同様な暗号化スイッチを設けることで容易に実現できる。さて、暗号化された入力データは、暗号化されたことを示す信号を子局制御部１１４から付加されて子局送信データスクランブル化処理部１０４に送られる。子局送信データスクランブル化処理部１０４では、あらかじめ定められたパターンの符号で暗号化された入力データがランダム化され、子局送信データ処理部１０５でパケット化され、子局送信部１０６で無線変調される。無線変調された信号は、子局送受信切り換えスイッチ１０７から、子局アンテナ１０８に送られ無線電波として送出される。また、暗号化使用／未使用選択部１１３で暗号化未使用が選択されているときは、入力データは暗号化されず、そのままスクランブル以下の処理を受けて送出される。

【０００８】子局アンテナ１０８から送出された無線電波は、ネットワーク側親局装置２００の親局アンテナ２０８で受信され、親局送受信切り換えスイッチ２０７で親局受信部２０９に送られ、復調される。復調出力は親局受信データ処理部２１０でパケットの解体処理が行われ、親局受信データスクランブル解除処理部２１１で、子局送信データスクランブル化処理部１０４でスクランブル化したのと同じパターンの符号によりスクランブルが解除される。スクランブルを解除された信号は、親局受信データ暗号化解読処理部２１２に送られる。親局制御部２１４は、受信した信号に暗号化処理を行ったことを示す信号が含まれていると、暗号化管理テーブル２１３にその端末が暗号化を選択していることを登録し、あらかじめ用意されている当該端末の暗号解読キーを抽出し、親局受信データ暗号化解読処理部２１２で暗号化解読処理を行って通常のデータを取り出し、ネットワークインタフェース２０２を経由し、イーサネット（登録商標）あるいはＡＴＭのネットワーク２０１に送出する。また、受信した信号に暗号化処理を行ったことを示す信号が含まれていないときは、暗号化管理テーブル２１３にその端末が暗号化を選択していないことを登録し、親局受信データ暗号化解読処理部２１２で暗号化解読処理を行わずに、スクランブルを解除したデータをネットワークインタフェース２０２を経由し、ネットワーク２０１に送出する。

【０００９】ネットワーク側親局装置２００からデータを送信する場合は、ネットワーク２０１からのデータがネットワークインタフェース２０２を経由し、親局送信データ暗号化処理部２０３に送られる。親局制御部２１４は、送出される相手子局が、暗号化使用を選択しているかどうかを、暗号化管理テーブル２１３でチェックし、暗号化が選択されていると、あらかじめ用意された相手子局に割り当てられている暗号化キーを抽出し、親局送信データ暗号化処理部２０３を動作させ、入力データを暗号化する。暗号化されたデータには、暗号化されていることを示す信号が付加されて、親局送信データスクランブル化処理部２０４に送られる。親局送信データスクランブル化処理部２０４では、あらかじめ定められたパターンの符号でデータがランダム化され、親局送信データ処理部２０５でパケット化され、親局送信部２０６で無線変調される。無線変調された信号は、親局送受信切り換えスイッチ２０７から、親局アンテナ２０８に送られ無線電波として送出される。また、暗号化管理テーブル２１３上で送信相手の子局が暗号化を選択していないことが登録されていると、上記の暗号化処理は行われない。

【００１０】親局アンテナ２０８から送出された無線電波は、子局アンテナ１０８で受信され、子局送受信切り換えスイッチ１０７で子局受信部１０９に送られ、復調される。復調出力は子局受信データ部１０５でパケットが解体処理され、子親局受信データスクランブル解除処理部１１１で、スクランブルが解除される。スクランブルを解除された信号は、子局受信データ暗号化解読処理部１１２に送られる。子局制御部１１４は、受信した信号に暗号化処理を行ったことを示す信号が含まれていると、自分の暗号化キーを用いて子局受信データ暗号化解読処理部１１２で暗号化解読処理を行い、端末インタフェース１０６を経由し、入出力装置１０１に出力する。

【００１１】以下でより詳細な説明を行う。まず、無線ＬＡＮによく使用される伝送フレームを図３を用いて説明する。この伝送フレームは、子局に対し親局の動作タイミングを報知し、親局から子局に対し各種制御情報を通知する報知チャネル、子局から親局に対し各種制御情報を通知する要求チャネル、親局から子局に対し通信許可を通知し、親局から子局に対し各種制御情報を通知する許可チャネル、親局から特定の子局に対し、または、特定の子局から親局に対しデータを送信するデータチャネル、データ信号の受信に対する応答としてＡＣＫ／ＮＡＫを送信する受信確認チャネルの各チャネルから構成されている。このフレーム構成で、子局は、送信データが発生すると、親局にたいし、要求チャネルで送信許可を求め、親局は許可チャネルで子局に通信を許可し、使用するデータチャネルの番号を指定する。そして子局は指定されたデータチャネルでデータを送信するというプロトコルで通信を行っている。また、親局からの送信

は、子局に、許可チャネルを介してこれからデータを送ることを伝え、使用するデータチャネルを指示し、子局は指示されたデータチャネルでデータを受信する。ここでは、要求チャネルと許可チャネルはそれぞれ１チャネルしかないと仮定する。また各チャネルの先頭には、図３に示すように、ガードタイム、ビット同期信号、フレーム同期信号、識別信号、チャネル情報、暗号化情報等からなるヘッダを含んでいる。

【００１２】上記の伝送フレーム構成で、暗号化が選択されているときに暗号化の対象となるのはデータチャネルのヘッダを除いたデータ部のみであり、一方、スクランブルは各チャネルとも、ヘッダ内のチャネル情報、暗号化情報等とそれに続く情報が対象となる。そして、子局側で暗号化を選択しているか否か、親局の暗号管理テーブルで暗号化が登録されているかを各送信時に相手局へ伝えるために、要求チャネル、許可チャネル、データチャネルの先頭部に暗号化あり／なしの暗号化フラグを暗号化情報として挿入するものとする。受信側の制御部１１４または２１４は、このフラグを見て暗号解読を行うか否かを判定する。

【００１３】親局に設けられた暗号化管理テーブル２１３は、データチャネルで子局へデータを送信する場合には、その暗号化管理テーブルから該当する子局の暗号化の情報を読みだして送信データの暗号化を行って送信するか、そのまま送信するかをを決めるのに用いられるが、各子局に関する情報は、その子局に割り当てられている暗号化キーと暗号解読キーと暗号化を選択しているかどうかを示すフラグよりなる。暗号化キーは暗号化する場合に使用し、暗号解読キーは暗号解読に使用するが、暗号化の方式によっては、暗号化キーと暗号解読キーは同じものである場合もある。暗号化管理テーブルで、子局が暗号化を選択しているかどうかを示す情報は、子局が送信要求時に要求チャネルに付加した前記暗号化フラグをテーブル２１３へ登録したものである。すなわち、暗号化を選択したときは、暗号化フラグは例えば“１”、暗号化を選択しないときは“０”とする。

【００１４】図４は、子局から親局へデータを送信する場合の、制御部１１４及び制御部２１４により実行される制御フローである。いま子局１で送信データが発生すると（ＳＴＥＰ１０）、子局１は、図１の暗号化使用／未使用選択部１１３を見て、暗号化スイッチが暗号化状態であるかを見る（ＳＴＥＰ１１）。すなわち、ユーザは送信データを暗号化して送信する場合には、あらかじめ、暗号化使用／未使用選択部１１３の暗号化スイッチをＯＮにしておくものとする。もし暗号化スイッチがＯＦＦなら（ＳＴＥＰ１１でＮＯ）、図３の要求チャネルの先頭部にあるチャネル情報、暗号化情報等を示すエリアに暗号化フラグをたてずに、要求チャネルを親局に送信する（ＳＴＥＰ１３）。もし暗号化スイッチがＯＮなら（ＳＴＥＰ１１でＹＥＳ）、図３の要求チャネルの先頭部にあるチャネル情報、暗号化情報等を示すエリアに暗号化フラグをたて、要求チャネルで親局に送信する（ＳＴＥＰ１２）。要求チャネルでデータの送信を要求した子局１は、許可チャネルで自局宛の信号が受信されるのを待つ（ＳＴＥＰ１４でＮＯのループ）。

【００１５】一方、親局は、要求チャネルで子局からの信号の受信を待っていて（ＳＴＥＰ２０でＮＯのループ）、子局１からの要求チャネルの信号を受信すると（ＳＴＥＰ２０でＹＥＳ）、図１の暗号化管理テーブル２１３の子局１のエリアに要求チャネルで送られてきた暗号化フラグの状態を書き込む（ＳＴＥＰ２２）。例えば、子局１が暗号化を選択している場合は、暗号化フラグの状態は“１”で、暗号化を選択していなければ“０”である。もし暗号化フラグが“１”なら（ＳＴＥＰ２２でＹＥＳ）、使用するデータチャネルを指定する許可チャネルで暗号化フラグを立てた信号を子局１に送信する（ＳＴＥＰ２３）。もし、暗号化フラグが“０”なら（ＳＴＥＰ２２でＮＯ）、許可チャネルで暗号化フラグをたてずに送信する（ＳＴＥＰ２４）。許可チャネルで自局宛の信号を待っていた子局１は、親局からの許可チャネルの信号を受信すると（ＳＴＥＰ１４でＹＥＳ）、受信した許可チャネルの信号に暗号化フラグが立っているかを見る（ＳＴＥＰ１５）。暗号化フラグが立っていれば（ＳＴＥＰ１５でＹＥＳ）、図１の子局送信データ暗号化処理部１０３で、送信データを自局に割り当てられた暗号化キーをもとにして暗号化し（ＳＴＥＰ１６）、データチャネルの先頭部にあるチャネル情報、暗号化情報を示すエリアに暗号化の状態を示すフラグを立てて、許可チャネルで指示されたデータチャネルで暗号化したデータを送信する（ＳＴＥＰ１７）。要求チャネルに暗号化フラグが立っていなければ、送信データを暗号化しないで（ＳＴＥＰ１８）、データチャネルの先頭部に暗号化フラグを立てずに送信する（ＳＴＥＰ１９）。親局からは、要求チャネルで信号に暗号化フラグが立っていれば、許可チャネルでも暗号化フラグを立てて送信するので、通常は、要求チャネルで暗号化フラグを立てたのに、その応答である許可チャネルで暗号化フラグが立っていない信号が受信されることはない。

【００１６】親局では、許可チャネルの信号で、子局１にデータ送信に使用するデータチャネルを指定するので、親局は子局１に指定したデータチャネルで受信を待っている（ＳＴＥＰ２５でＮＯのループ）。子局１からのデータを受信すると（ＳＴＥＰ２５でＹＥＳ）、そのデータチャネルの先頭部で暗号化フラグが立っているかをみて（ＳＴＥＰ２６）、フラグが立っていれば（ＳＴＥＰ２６でＹＥＳ）、図１の親局受信データ暗号化解読処理部（２１２）で暗号解読の処理を行う（ＳＴＥＰ２７）。もし、データチャネルの先頭部に暗号化フラグが立っていなければ（ＳＴＥＰ２６でＮＯ）、暗号化解読処理は行わず、そのまま受信する。暗号化されたデータ

の解読は、暗号化管理テーブル２１３の子局１のエリアにある暗号解読キーを用いて行う。

【００１７】図５は、親局から子局にデータを送信する場合に各制御部１１４、２１４で実行される制御フローである。親局で、子局１に送る送信データが発生すると（ＳＴＥＰ３１）、図１の暗号化管理テーブル２１３の子局１のエリアに暗号化フラグが立っているかを見る（ＳＴＥＰ３２）。暗号化フラグが立っていれば、子局１は暗号化の送受信を選択していると判断し、許可チャネルで暗号化フラグを立てて、子局１に信号を送信し（ＳＴＥＰ３３）、送信データを暗号化管理テーブル２１３の子局１のエリアに記憶してある暗号化キーを用いて、親局送信データ暗号化処理部２０３で暗号化し（ＳＴＥＰ３４）、データチャネルで、暗号化フラグを立てて、暗号化したデータを子局１に送信する（ＳＴＥＰ３５）。またもし、暗号化管理テーブル２１３で、子局１の暗号化フラグが立っていなければ（ＳＴＥＰ３２でＮＯ）、暗号化フラグを立てずに許可チャネルを送信し（ＳＴＥＰ３６）、親局送信データ暗号化処理部２０３で暗号化せず（ＳＴＥＰ３７）、データチャネルで暗号化フラグも立てずに送信データを子局１に送信する（ＳＴＥＰ３８）。

【００１８】子局は、許可チャネルで親局からの自局への送信信号を常時受信している（ＳＴＥＰ４１でＮＯのループ）。許可チャネルで、自局への信号が受信されたら（ＳＴＥＰ４１でＹＥＳ）、許可チャネルに暗号化フラグが立っているかを見る（ＳＴＥＰ４２）。もし立っていれば（ＳＴＥＰ４２でＹＥＳ）、暗号化解読の準備をして（ＳＴＥＰ４３）、データチャネルでのデータ受信を待つ（ＳＴＥＰ４４でＮＯのループ）。暗号化解読の準備としては、自局に割り当てられた暗号解読キーを抽出し、子局受信データ暗号化解読処理部１１２の駆動を準備する。データチャネルで親局からのデータが受信されたら（ＳＴＥＰ４４でＹＥＳ）、子局受信データ暗号化処理部１１２で暗号化されたデータを解読し受信する（ＳＴＥＰ４５）。受信した許可チャネルの信号に暗号化フラグが立っていなければ（ＳＴＥＰ４２でＮＯ）、非暗号化解読の準備をして（ＳＴＥＰ４６）、データチャネルでの受信を待つ（ＳＴＥＰ４７でＮＯのループ）。非暗号化解読の準備としては、子局受信データ暗号化解読処理部１１２の処理をスキップさせるための準備である。親局からのデータがデータチャネルで受信されたら（ＳＴＥＰ４７でＹＥＳ）、子局受信データ暗号化解読処理部１１２の解読処理を行わずデータを受信する（ＳＴＥＰ４８）。本子局の制御フローでは、許可チャネルでの暗号化フラグで、親局からのデータの暗号化解読を行うか、行わないかを決めたが、親局から送信されるデータチャネルにも暗号化フラグが含まれているので、そのフラグで暗号化解読の操作を行うかどうかを決めてもよい。

【００１９】以上、図４と図５の制御フローでは、子局１からのデータ送信と、親局から子局１に対するデータ送信について、データの暗号化が選択できる方法についてのみ説明したが、実際の送受信には、図３の伝送フレームに示すように、データ送信後には、各チャネルでの送信が正しく相手に伝わったかの受信確認チャネルでのＡＣＫ／ＮＡＫ信号による確認が行われ、ＮＡＫの場合にはデータの再送なども行われるが、これらの制御については説明を省略する。また、図１の構成では、子局送信データ暗号化処理部１０３や親局送信データ暗号化処理部２０３で送信データの暗号化を行った後に、子局送信データスクランブル化処理部１０４や親局送信データスクランブル化処理部２０４で、送信データのスクランブル化を行っているが、スクランブル化も一種の暗号化であり、ＤＥＳやＦＥＡＬなどの暗号化キーを用いた強力な暗号化を行ったあとのデータを再度スクランブル化することは、必ずしも必要ない。スクランブル化処理部のない構成も十分実用になると考えられる。

【００２０】以上詳細に説明したように、本発明では、子局に暗号化を行うか行わないかの選択ができるスイッチを設け、ユーザは、送信データが暗号化を必要とするデータかどうかを判断して、暗号化が必要としたデータ送信の場合にのみ、暗号化を行い、暗号化が不要と判断した場合は、暗号化を行わずにデータを送信し処理の高速化を図る。一方、親局には、管理テーブルを設け子局が暗号化を選択したかどうかを記憶し、親局からのデータ送信は、この管理テーブルに記憶している子局の状態に従って暗号化するかどうかを定める。送信されたデータが暗号化されているかどうかは、データチャネルや許可チャネルの信号の先頭に暗号化フラグを立てるか立てないかで受信側に容易に知らせることができる。

【００２１】

【発明の効果】本発明により、以下の効果がある。

（１）暗号化が必要なデータのみ暗号化を行うので、暗号化を行う必要のないデータの処理が遅くなることがなく、処理の遅れにともなう不快感のない通信ができる。

（２）暗号化を行う場合が少なくなるので、暗号方式として、処理がかかる強力な方式も採用することができ、無線区間を傍受された場合のデータの秘匿能力が高まる。

【図面の簡単な説明】

【図１】本発明になる無線ＬＡＮシステムの構成例を示すブロック図である。

【図２】無線ＬＡＮシステムの説明図である。

【図３】無線ＬＡＮシステムの伝送フレームの例を示す図である。

【図４】子局送信の場合の制御フローである。

【図５】親局送信の場合の制御フローである。

【符号の説明】

１０３　子局送信データ暗号化処理部

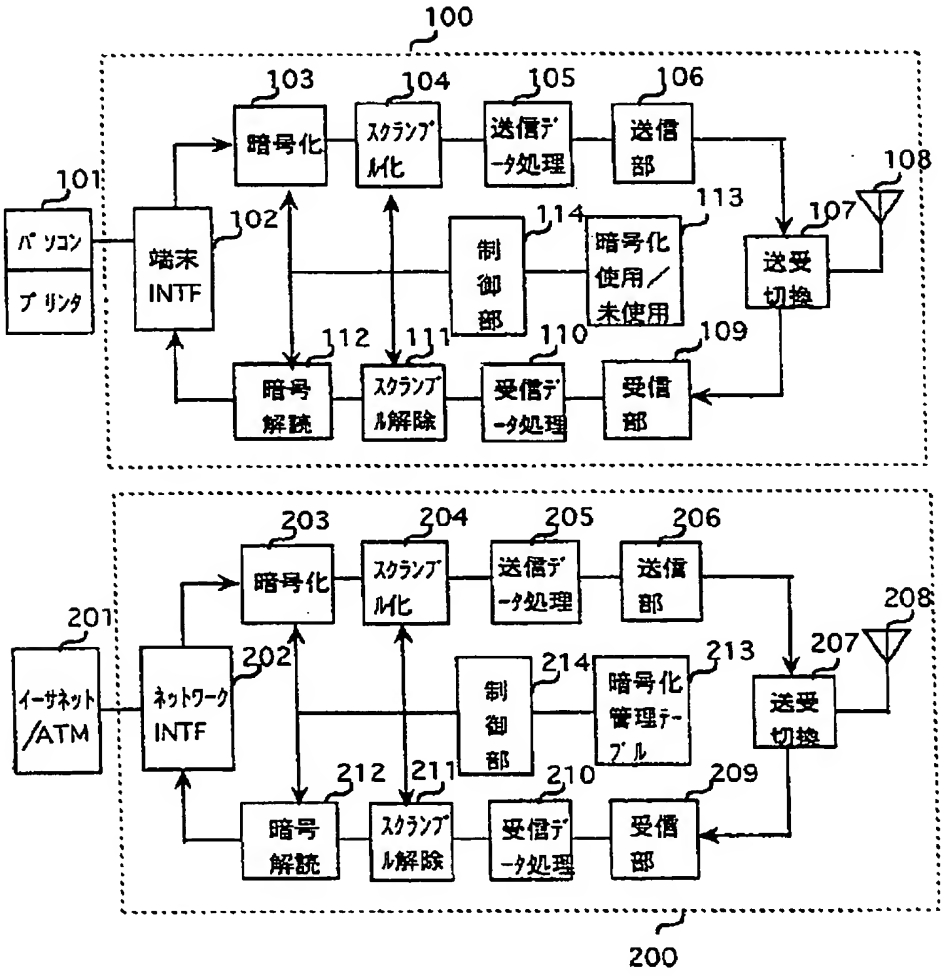
11

１０４　子局送信データスクランブル化処理部
１０５　子局送信データ処理部
１０６　子局送信部
１０９　子局受信部
１１０　子局受信データ処理部
１１１　子局受信データスクランブル解除処理部
１１２　子局受信データ暗号化解読処理部
１１３　暗号化使用／未使用選択部
１１４　子局制御部
２０２　ネットワークインタフェース

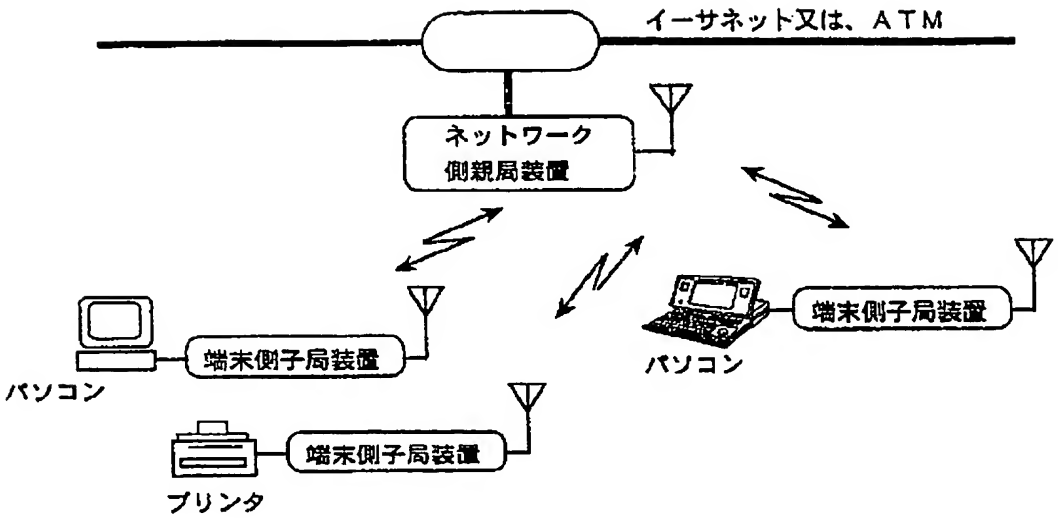
12

２０３　親局送信データ暗号化処理部
２０４　親局送信データスクランブル化処理部
２０５　親局送信データ処理部
２０６　親局送信部
２０９　親局受信部
２１０　親局受信データ処理部
２１１　親局受信データスクランブル解除処理部
２１２　親局受信データ暗号化解読処理部
２１３　暗号化管理テーブル
２１４　親局制御部

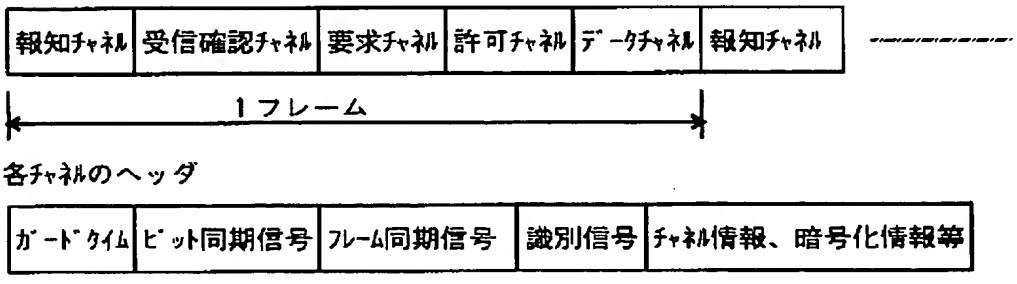
【図１】



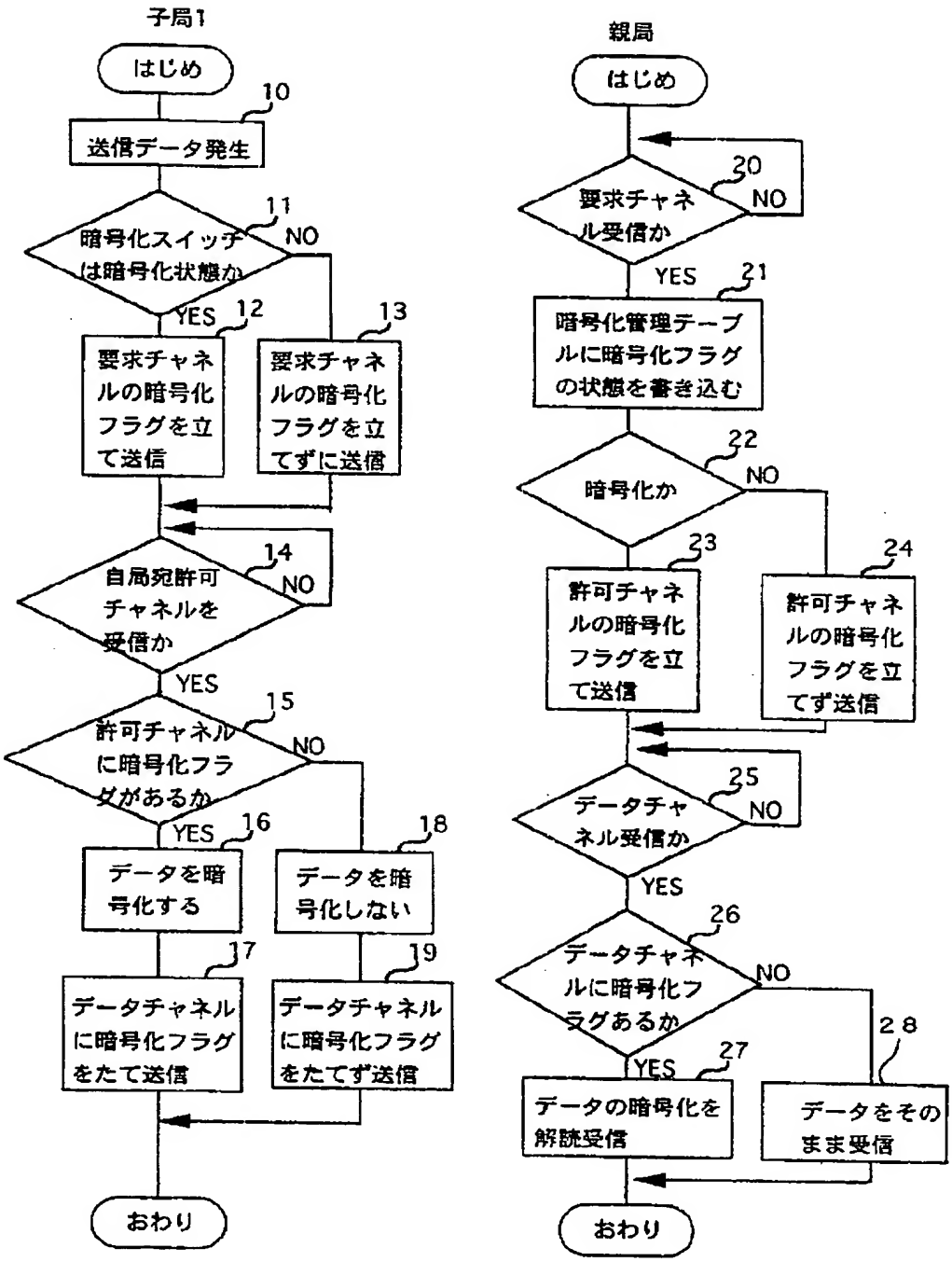
【図２】


イーサネット又は、ＡＴＭ
ネットワーク
側親局装置
端末側子局装置
パソコン
端末側子局装置
パソコン
端末側子局装置
プリンタ

【図３】

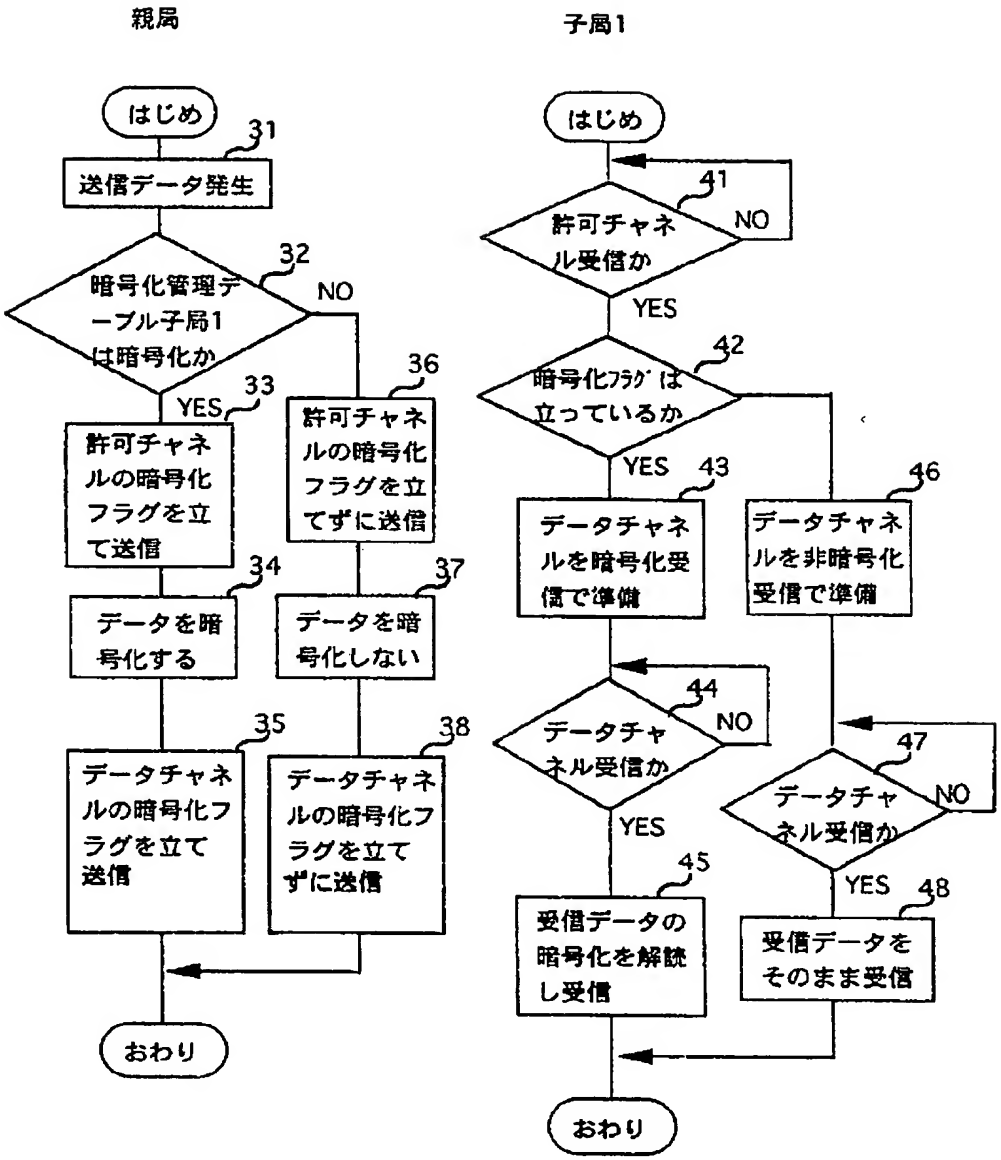

報知ﾁｬﾈﾙ
受信確認ﾁｬﾈﾙ
要求ﾁｬﾈﾙ
許可ﾁｬﾈﾙ
ﾃﾞｰﾀﾁｬﾈﾙ
報知ﾁｬﾈﾙ
１フレーム
各ﾁｬﾈﾙのヘッダ
ｶﾞｰﾄﾞﾀｲﾑ
ﾋﾞｯﾄ同期信号
ﾌﾚｰﾑ同期信号
識別信号
ﾁｬﾈﾙ情報、暗号化情報等

【図４】



子局から親局へのデータ送信時の制御フロー

【図５】



親局から子局へのデータ送信時の制御フロー

フロントページの続き

(72)発明者　沖野　恵美
東京都中野区東中野三丁目14番20号　国際電気株式会社内

(72)発明者　三浦　俊二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　鈴木　芳文
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考) 5B089 GA21 GA31 GB01 HA06 HA11
KA05 KA17 KB13 KC15 KC22
KC37 KH30
5J104 AA01 PA01
5K033 AA02 AA08 CB01 DA01 DA17
DB10 DB12 DB14
5K067 AA30 AA35 BB21 EE22 EE42
HH36 KK13